I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Behavioral Targeting: Issues Involving the Microsoft-aQuantive and Google-DoubleClick Mergers, and the Current and Proposed Solutions to Those Issues

JAMES SCHEDWIN*

ABSTRACT: Behavioral targeting is a method used by online advertisers to collect information on Internet users in order to better target their advertising toward those users. Concerns exist in this field regarding the protection and security of the information collected. Such concerns have become amplified after recent mergers between companies with large databases of behavioral information, such as the Microsoft-aQuantive and Google-DoubleClick mergers of 2007 and 2008. This note serves as an overview of the issues raised by mergers between companies with databases of behavioral information, and specifically addresses the concerns raised by such mergers, the current regulatory system in place regarding behavioral targeting information, and proposed methods regarding the future regulation of behavioral targeting.

* James Schedwin is a 2009 Juris Doctor candidate at Moritz College of Law at The Ohio State University. He received a Bachelor of Arts from The Ohio State University in 2005.

I. INTRODUCTION

Behavioral targeting is a practice that online advertising companies use to place advertisements that consumers are likely to be receptive towards. While considered an effective and innovative method of advertising, behavioral advertising primarily targets consumers by collecting potentially sensitive data on persons via their website visits and Internet searches.

Privacy groups began expressing concerns about behavioral targeting around the time of the failed DoubleClick-Abacus merger in 2001, leading to such enforcement as the National Advertising Initiative's self-policing agreement (the "NAI Agreement"). Currently, behavioral targeting issues have been revived due to the recent mergers of Microsoft-aQuantive and particularly Google-DoubleClick as a result of the large amount of data being merged and concerns over the current regulatory structure.

This note discusses the privacy concerns raised by these mergers. First, the article explains behavioral targeting and the privacy concerns it creates. The article then discusses the DoubleClick-Abacus, Microsoft-aQuantive, and Google-DoubleClick mergers and their significance to behavioral targeting. The article then describes the Federal Trade Commission's new proposed principles regarding behavioral targeting, as well as the critiques and responses these principles have generated. The article concludes with a brief discussion of the Federal Trade Commission's February 2009 revised principles regarding behavioral targeting.

II. WHAT IS BEHAVIORAL TARGETING AND WHY DOES IT POSE PRIVACY CONCERNS

Behavioral targeting is the process by which advertisers track Internet users' online activities and place ads based on these activities.[1] Typically, the advertisers create behavioral segments to describe users' online activities, and then, when the user visits other

---

[1] Specific Media, *What is Behavioral Targeting?*, http://www.behavioraltargeting.com/what-is-behavioral-targeting.html (last visited Feb. 1, 2009). According to the Federal Trade Commission's proposal for self-regulatory guidelines, behavioral targeting is "the tracking of a consumer's activities online to target advertising." FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2007) [hereinafter ONLINE BEHAVIORAL ADVERTISING], http://www.ftc.gov/os/2007/12/P859900stmt.pdf.

sites, the advertisers place ads for products that relate to the behavioral segment with which the user is identified.[2] Information from Internet users is gathered by tracking the websites they visit, the keyword searches they conduct, and also by profiling visitors to a customer's website and then tracking his or her behavior.[3] This information is then used to identify advertisers' target audiences and place ads for products based on where a person has gone or what a person has done online, creating more personally directed advertisements.[4] This information collection and tracking is largely done via "cookies."

Cookies are small files deposited on the hard drive of a user as the user navigates the Internet.[5] Cookies track what a person is doing online, and while they can improve a website by making it easier for the user to navigate or customize the site, cookies can also profile and track the behavior of a user when they are online.[6] Major online advertisers use cookies in order to learn of the web-browsing habits of users, and target those users with advertisements that are potentially more relevant to a particular consumer.[7]

The debate about the lack of privacy in online advertising revolves around the use of tracking devices such as cookies. The concerns over the use of cookies stems from the fact that cookies can follow a user through countless websites and can do so for long periods of time, potentially decades.[8] In order to prevent these information-gathering practices, some companies that use cookies "abide by a self-regulation

---

[2] Specific Media, *supra* note 1. Behavioral segments are usually based on activities of a user online, such as what sites he or she has visited and what keyword searches he or she has performed.

[3] *Id.*

[4] Joshua Koran, *Understand the 4 BT Methods*, IMEDIA CONNECTION, July 18, 2008, http://www.imediaconnection.com/content/consumer-strategies-targeting-understand-the-4-bt-methods-_19935.html; Russell Shaw, *Behavioral Targeting 101*, IMEDIA CONNECTION, Apr. 28, 2004, http://www.imediaconnection.com/content/3297.asp.

[5] Pam Dixon, *Consumer Tips: How to Opt-Out of Cookies That Track You*, WORLD PRIVACY FORUM, Sept. 1, 2004, http://www.worldprivacyforum.org/cookieoptout.html.

[6] *Id.*

[7] FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS 6–8 (June 2000) [hereinafter FTC REPORT TO CONGRESS], http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf.

[8] *Id.*

scheme that asks [a user] for consent [to use the cookies] in some cases and offers an opt-out [cookie for] this kind of tracking."[9] The self-regulatory scheme in question was formalized in the NAI Agreement, which will be discussed in further detail below.[10]

Behavioral targeting poses a threat to privacy by allowing advertisers to use tracking to collect sensitive personal data from unknowing Internet users. Advertisers, in order to personalize their advertisements to individual users, need to gather and store information based on an individual's web activities.[11] Storage of collected personal information has led to the creation of large databases containing Internet-use information on millions of Internet users, diminishing the privacy of consumers significantly by potentially allowing third parties, such as law enforcement agents, to survey the databases without any legal basis.[12]

III. THE DOUBLECLICK-ABACUS MERGER AND FTC/NAI AGREEMENT

DoubleClick is one of the largest and most successful online advertising companies in the world, having amassed a large database of personal information via behavioral targeting, including data such as a web surfer's shopping habits and website visits.[13] The amount of data collected, and its personal nature, has created a high level of concern from organizations such as the Electronic Privacy Information Center ("EPIC"), particularly in regard to the security of the data collected and the unstated uses of the data gathered.[14] This

---

[9] *Id.*

[10] The NAI adopted new principles of self-regulation in December of 2008. See Part VII, *infra*, for a discussion of these newly adopted principles.

[11] FTC REPORT TO CONGRESS, *supra* note 7, at 5. DoubleClick, in particular, tracks individuals through the Internet by assigning users a unique number and recording that number in a cookie on the user's computer. The user is then recorded as visiting other sites where DoubleClick serves ads, which is stored by DoubleClick for two years. *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, In Re Google and DoubleClick, at 9 (Fed. Trade Comm'n, Apr. 20, 2007), http://epic.org/privacy/ftc/google/epic_complaint.pdf.

[12] *In Re Google and DoubleClick*, *supra* note 11, at 10.

[13] Patricia Jacobus, *FTC Investigates DoubleClick's Data-Collection Practices*, CNET NEWS, Feb. 16, 2000, http://news.cnet.com/2100-1023-237007.html.

[14] *In Re Google and DoubleClick*, *supra* note 11, at 1–2.

concern, and concerns in general regarding behavioral targeting advertisers, is prevalent because of the combination of large amounts of personally and non-personally identifiable data because of mergers between companies that each had gathered a significant store of data on Internet users.[15] Critics noted such concern with the DoubleClick-Abacus merger of 1999.

DoubleClick's merger with Abacus was the first merger to create extensive privacy concerns. In 1999, DoubleClick and offline market researcher Abacus gained shareholder approval to merge.[16] The purported aim of the merger was to allow the combined company to target potential consumers with greater accuracy by using the customers' online viewing tendencies to offer advertisements specifically directed to customers' interests.[17] The merger was to combine DoubleClick's information from its five billion Internet ads per week with Abacus's two billion personally identifiable consumer catalog transactions, a merger of two large databases.[18]

Privacy groups were opposed to the proposed merger due to the potential that the combined company would abuse the personal data gathered by the newly formed company.[19] Among these groups were Junkbusters, EPIC, Privacy International, and the U.S. Public Interest Research Group.[20] The stock market also reacted unfavorably to the deal; news of the merger agreement caused the value of both DoubleClick and Abacus stock to decline, with DoubleClick's stock dropping primarily due to privacy concerns including a formal investigation opened by the Federal Trade Commission ("FTC") and inquires by attorneys general concerning DoubleClick's business

---

[15] *Id.* at 10.

[16] Courtney Macavinta, *DoubleClick, Abacus Merge in $1.7 Billion Deal,* CNET NEWS, Nov. 24, 1999, http://www.news.com/2100-1023-233526.html.

[17] *Id.*

[18] *Id.*

[19] *Id.*; *see also* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 1.

[20] Computergram Int'l, *Privacy Fallout from DoubleClick Merger with Abacus Direct,* CBR ONLINE, June 22, 1999, http://www.cbronline.com/news/privacy_fallout_from_doubleclick_merger_with_abacus_direct.

practices.[21] Additionally, the FTC required DoubleClick to adopt privacy standards for online advertising and to create an opt-out cookie that would note users who did not desire to receive advertising through DoubleClick.[22] Although the merger was consummated, DoubleClick eventually sold Abacus at a financial loss after the FTC was asked to get involved and force DoubleClick's adoption of privacy standards.[23] DoubleClick admitted that it made a "mistake by planning to merge names with anonymous user activity across websites in the absence of government and industry privacy standards," a mistake the stock market recognized immediately with the aforementioned decrease in stock value.[24]

After the DoubleClick-Abacus fiasco, the FTC entered into an agreement with several online advertising companies regarding privacy-supporting practices, adopted by those advertisers as members of the Network Advertising Initiative.[25] The NAI Agreement addressed behavioral targeting companies' concerns over stringent regulation fears, and attempted to alleviate concerns about privacy in mergers between companies with offline data and those with online information.[26] Under the NAI Agreement, companies receive a safe

---

[21] *DoubleClick, Abacus Stocks Drop After Merger News*, DIRECT MAG., June 15, 1999, http://directmag.com/news/marketing_doubleclick_abacus_stocks; Mark Sakalosky, *DoubleClick's Double Edge*, CLICKZ, Sept. 3, 2002, http://www.clickz.com/1455141.

[22] *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry: What are the Risks for Competition and Privacy? Before the S. Subcomm. on Antitrust, Competition Policy, and Consumer Rights of the S. Comm. on the Judiciary*, 110th Cong. 2 (2007) (statement of Marc Rotenberg, President, Electronic Privacy Information Center), http://epic.org/privacy/ftc/google/epic_test_092707.pdf.

[23] *Id.*; *see also* David A. Utter, *DoubleClick Dumps Abacus at a Loss*, WEBPRONEWS, Dec. 28, 2006, http://www.webpronews.com/topnews/2006/12/28/DoubleClick-dumps-abacus-at-a-loss.

[24] *An Examination of the Google-DoubleClick Merger and the Online Advertising Industry*, *supra* note 22; Utter, *supra* note 23.

[25] PAM DIXON, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION 5 (2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf. *See also* Network Adver. Initiative, A Track Record of Success, http://www.networkadvertising.org/about/history.asp (last visited Feb. 2, 2009).

[26] Press Release, Fed. Trade Comm'n, Federal Trade Commission Issues Report on Online Profiling (July 27, 2000), *available at* http://www.ftc.gov/opa/2000/07/onlineprofiling.shtm. The NAI principles agreed to were as follows: (1) consumers were to be given notice of the profiling activities of network advertisers along with a choice not to participate; (2) choice, which involved a question of

harbor against any new federal privacy legislation, provided the companies keep the FTC informed about their actions, and that they follow NAI guidelines. [27] This agreement represented the first regulation of behavioral tracking to reach DoubleClick and their business practices, as DoubleClick joined and is now currently a member of the NAI as part of Google.[28] Still, proposed legislation from policymakers and criticisms by consumer advocate groups indicated that the NAI Agreement was likely just the start of the regulation of behavioral targeting.[29] However, the principles set forth in the NAI Agreement did provide relief among the advertising companies that such enforcement was going to be a gradual process.[30]

IV. THE MICROSOFT-AQUANTIVE MERGER

On May 18, 2007, Microsoft issued a press release stating that it agreed to acquire aQuantive, an online advertising platform. [31]

---

opt-in and opt-out options for users in regard to the sensitivity of the information that was being collected; (3) access provided to users regarding information that was or was related to personally identifiable information; (4) reasonable efforts to keep the data collected secure by network advertisers; (5) NAI companies would agree to have violations enforced by a third party enforcement program, with NAI companies submitting to independent compliance audits with public results if this was not done in six months.

[27] Keith Perine, *Who Are the Privacy Police?– Government Activity*, THE INDUS. STANDARD, Aug. 14, 2000, *available at* http://findarticles.com/p/articles/mi_moHWW/is_30_3/ai_66678711/pg_1. The NAI was granted the ability to implement safe harbors to self-regulatory principles that effectively implemented fair information practices articulated within legislation and any subsequent rules made. The final decision as to whether any self-regulatory guidelines qualify for safe harbor status would be made by the NAI following any rulemaking, after the NAI had an opportunity to evaluate the effectiveness of the guidelines at the time the safe harbor application was made. FTC REPORT TO CONGRESS, *supra* note 7, at 10–11.

[28] Network Adver. Initiative, Opt Out of NAI Member Ad Networks, http://www.networkadvertising.org/managing/opt_out.asp (last visited Feb. 2, 2009). The former DoubleClick opt-out no longer exists, having been replaced by a Google opt-out cookie.

[29] DIXON, *supra* note 25, at 1; Stefanie Olsen, *Ad Firms Benefit from FTC Privacy Decision*, CNET NEWS, July 28, 2000, http://att.com.com/Ad-firms-benefit-from-FTC-privacy-decision/2100-1023_3-243822.html.

[30] Olsen, *supra* note 29.

[31] Press Release, Microsoft Adver. Worldwide, Microsoft to Acquire aQuantive, Inc. (May 18, 2007), *available at* http://advertising.microsoft.com/asia/NewsAndEvents/PressRelease.aspx?Adv_PressReleaseID=537.

Microsoft completed the acquisition on August 13, 2007; the deal represented the most expensive acquisition in Microsoft's history, costing over six billion dollars.[32] The aQuantive acquisition was one of many acquisitions that Microsoft made in its effort to expand its online advertising reach in response to Google's growing presence in online advertising.[33]

Microsoft began aggressively competing against Google in 2003 in online search and advertising.[34] At the time of the Microsoft-aQuantive merger, advertisement dollars had been moving online and Google had become an advertising powerhouse.[35] Indeed, many speculated that Microsoft paid such a high price for aQuantive because it was desperate to stay competitive with Google in the online advertising business.[36] Microsoft needed a way to allow it to deliver content and advertising online, and it could do both by acquiring aQuantive.[37] This merger was akin to the Google-DoubleClick merger described in the next section, and thus implicates similar privacy concerns regarding database mergers as will be discussed in the section below.

---

[32] The FTC approved the acquisition on July 6, 2007. Thomas Claburn, *FTC Clears Microsoft's $6 Billion Deal for aQuantive*, INFO. WEEK, July 9, 2007, http://www.informationweek.com/news/showArticle.jhtml?articleID=200900868&subSection=All+Stories; John Fontana, *Microsoft Buys aQuantive, Sets Up Online Ad Group*, PC WORLD, Aug. 14, 2007, http://www.pcworld.com/printable/article/id,135928/printable.html.

[33] Fontana, *supra* note 32. Microsoft had also purchased AdCEN, which linked buyers and sellers of ad space, ScreenTonic, which delivered ads to mobile devices based on location, and Massive, which advertised through online video game services.

[34] Joe Wilcox, *Why Microsoft Wrote aQuantive a Big Check*, MICROSOFT WATCH, May 18, 2007, http://www.microsoft-watch.com/content/corporate/why_microsoft_wrote_aquantive_a_big_check.html.

[35] *Id.*

[36] Terence Channon, *Microsoft's aQuantive Deal: An Act of Desperation*, SEEKING ALPHA, May 21, 2007, http://seekingalpha.com/article/36090-microsoft-s-aquantive-deal-an-act-of-desperation. Privacy concerns were not cited as a major issue in the Microsoft-aQuantive merger, though this is possibly because larger databases were involved in the Google-DoubleClick merger.

[37] *Id.*

V. THE GOOGLE-DOUBLECLICK MERGER

The merger that has provoked the most concern about the privacy impacts of online behavioral targeting is the Google-DoubleClick merger, which the companies completed on March 11, 2008 after an acrimonious public debate.[38] In aligning with DoubleClick, Google stated it could "democratize display and rich-media ads the same way as it did with search, expanding the number of advertisers in the mix," or increasing the number of advertisers in a way to make display and rich-media ads more open, in turn boosting demand for the DoubleClick ad serving technology.[39] The merger was challenged by EPIC, the Center for Digital Democracy, and the U.S. Public Interest Research Group.[40] These groups asserted that the right to privacy is a fundamental right in the United States, and that right may be violated by the collection and use of personal information because Google and DoubleClick had yet to safeguard collected personal data adequately.[41]

Internet search engines are the primary way people access Internet content. Search terms such as those used in a Google search can reveal sensitive information on users, including their personal information and interests. In 2005 alone, over sixty million people used search engines.[42] DoubleClick collects data using "web bugs," also known as "clear GIFs," to collect data on Internet users.[43] In order to prevent web bugs or clear GIFs from collecting this personal data, a person must download an opt-out cookie to stop data

---

[38] Press Release, Google, Google Closes Acquisition of DoubleClick (Mar. 11, 2008), *available at* http://www.google.com/intl/en/press/pressrel/20080311_doubleclick.html.

[39] Stephanie Olsen, *Privacy Concerns Dog Google-DoubleClick Deal*, CNET NEWS, Apr. 18, 2007, http://news.cnet.com/Privacy-concerns-dog-Google-DoubleClick-deal/2100-1024_3-6177029.html.

[40] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 1–2.

[41] *Id.* at 1–3.

[42] *Id.* at 3.

[43] *Id.* at 4. "Web bugs," "clear GIFs," and "pixel tags" are incredibly tiny electronic tags featured on web pages, that act similar to beacons in that they send a call-back to a server stating that a user is on a website, and therefore, act as an alternative method to cookies of tracking users online. Concerns have been raised due to their nigh-undetectable nature, rendering most users unable to tell that data is being compiled on them when they are visiting websites. Stephanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET NEWS, July 12, 2000, http://news.cnet.com/2100-1017-243077.html.

collection.[44] However, most users are unaware of the need to download opt-out cookies, resulting in DoubleClick likely collecting data from the majority of Internet users.[45]

On April 20, 2007, EPIC, along with the other organizations challenging the Google-DoubleClick merger, filed a complaint (and subsequently filed two supplemental complaints) with the FTC, alleging violations of the FTC Act, and the Sherman and Clayton Antitrust Acts.[46] EPIC noted in its initial complaint that the Google-DoubleClick merger would allow Google to track both Internet search actions and website visits.[47] While Google already tracked search activity at the time of the proposed merger, it did not use the information it collected to engage in behavioral targeting.[48] Instead, Google stored search activity in connection with a person's Internet Protocol ("IP") address indefinitely, meaning Google could use such information to track search activity in the future.[49]

According to EPIC, DoubleClick created profiles of persons from users' web history of viewing sites that contained DoubleClick cookies and web bugs.[50] The information gathered by this technology was purportedly kept by DoubleClick's clients and DoubleClick had either

---

[44] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 5.

[45] DIXON, *supra* note 25, at 6.

[46] Electronic Privacy Information Center, Privacy? Proposed Google/DoubleClick Deal, http://epic.org/privacy/ftc/google/ (last visited Feb. 2, 2009). In its original complaint, EPIC challenged the merger under section 5 of the FTC Act, 15 U.S.C. § 45 (2008). Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 9–10. In its supplemental complaint, EPIC also challenged the merger under section 7 of the Clayton Antitrust Act, 15 U.S.C. § 18 (2008), as well as under section 1 of the Sherman Act, 15 U.S.C. § 1 (2008), which proscribe mergers that lessen competition and prohibite agreements constituting unreasonable restraints of trade, respectively. Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, In Re Google and DoubleClick, at 15 (Fed. Trade Comm'n Jun. 20, 2007), http://epic.org/privacy/ftc/google/supp_060607.pdf.

[47] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 6.

[48] *Id.* at 7.

[49] *Id.*

[50] *Id.* at 9. "Web bugs" are defined in footnote 42; "cookies" are defined in Section II, *infra*.

no or limited access to the data collected.[51] According to the complaint, DoubleClick gathered information without user awareness; users could not view the data collected on them, and while opt-out cookies were available from DoubleClick via the NAI, they still permitted the collection of "non-personally-identifiable information."[52] Furthermore, the opt-out cookies had to be downloaded again if a user purged cookies from his computer.[53]

EPIC claimed that Google was committing unfair or deceptive business practices in violation of Section 5 of the FTC Act.[54] EPIC argued that Google's privacy policy was not easily accessible to users, and that Google collected information from users without providing adequate notice.[55] EPIC noted in their complaint that Google collected information without complying with Fair Information Practices or Organization for Economic Co-operation and Development ("OECD") Privacy Guidelines, which was likely to cause substantial injuries to consumers that would not be reasonably avoidable by the consumers.[56] Such lack of reasonable avoidance was stated as causing likely substantial injuries through actions such as

---

[51] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46, at 1–2.

[52] *Id.* at 14. The NAI opt-out was formerly located on NAI's website. It is currently listed as a Google opt-out cookie, as Google and DoubleClick have merged. *See* Network Adver. Initiative, Opt Out of NAI Member Ad Networks, http://www.networkadvertising.org/managing/opt_out.asp (last visited Jan. 6, 2009).

[53] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46, at 14.

[54] *Id.* at 9. Section 5 of the FTC Act outlaws unfair methods, in or affecting commerce in competition, and unfair or deceptive acts in or affecting commerce. 15 U.S.C. § 45(a)(1) (2008). The term "unfair or deceptive practice" itself is not actually defined by the statute, or in the FTC Act, leaving the possibility that it is a broadly inclusive phrase. *See* Letter from Edolphus Towns, Congressman, to Deborah Platt Majoras, Chairman of the Fed. Trade Comm'n (Oct. 26, 2007), *available at* http://epic.org/privacy/ftc/google/towns_102607.pdf.

[55] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 9.

[56] *Id.* at 9–10. Fed. Trade Comm'n, Fair Information Practice Principles, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Feb. 2, 2009). Org. for Eco. Co-Operation and Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Feb. 2, 2009).

the storing of users' data without notice, and the undermining of the ability of consumers to avail themselves to privacy protections promised by behavioral targeting companies.[57] As such, injunctive relief was needed in order to prevent Google and DoubleClick from continuing to harm users through deceptive and unfair business practices.[58] EPIC thus concluded that the merger would create the largest database of Internet activities, and the lack of any legal obligation to privacy or security of the information required Google to show a public plan for compliance with guidelines, such as those of the OECD.[59] These guidelines required Google to give reasonable access to users whose data has been collected and maintained, to create a reasonable data destruction policy, and to have DoubleClick remove user identified cookies from their records before the merger unless given affirmative consent to keep them, in order to comply with the FTC and Antitrust Acts.[60]

EPIC filed two supplements to its complaint with additional facts on the merger in question.[61] The New York State Consumer Protection Board endorsed the original complaint, and expressed fear that Google and DoubleClick could create "superprofiles" of personally identifiable and non-identifiable information of web users, culminating in the largest such databases ever known.[62] Google's use

---

[57] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 10.

[58] *Id.* at 9. EPIC stated that the acts were deceptive because a user was not informed of Google's data collection processes until that user clicked through four links, and in doing so, allowed Google to collect user search terms and IP addresses without notice to the user. EPIC stated that the acts were unfair because they were performed without the knowledge or consent of users and without complying with Fair Information Practices and OECD Guidelines.

[59] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *supra* note 56.

[60] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 10–11.

[61] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46, at 1; *see also* Second Filing of Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Information and for Other Relief, In Re Google and DoubleClick, 1 (Fed. Trade Comm'n, Sept. 17, 2007), http://epic.org/privacy/ftc/google/supp2_091707.pdf.

[62] Supplemental Materials in Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46, at 2. "Personally identifiable information" is data that can be linked to specific individuals, including such examples as

of the various programs and devices it places online for people to use results in Google collecting data on persons that may be held for lengthy, indeterminate periods of time.[63] Among these programs and devices are *Orkut*, a social networking website, and *Google Calendar*, a scheduling tool that has its information maintained on Google's servers.[64] While Google claims data collection is used for "quality control" and "personalized user experiences," EPIC noted that Google never explained the meaning of "quality control."[65] Also, while Google does not sell user information, EPIC stated that Google has been known to share its information with other companies, and that Google's refusal to sell user information is merely a voluntary act.[66]

Despite the objections raised, on December 20, 2007, the FTC released a statement approving the Google-DoubleClick merger by a four to one vote.[67] The merger was reviewed under the Clayton Act, which prohibits a merger or acquisition that "may be substantially to lessen competition, or tend to create a monopoly."[68] In its opinion, the FTC noted that the merger was potentially harmful to Internet users because of the potential for the merged company to exploit its new, combined data set, but the FTC stated that it lacked authority to require conditions to the merger not relating to antitrust; the sole purpose of antitrust review being "to identify and remedy transactions that harm competition," and thus does not focus on harm to consumers.[69] Additionally, the FTC also stated that regulating one

---

e-mail, phone numbers, and addresses. "Non-identifiable information" is information based off of data on a consumer's computer sent by the cookie. FTC REPORT TO CONGRESS, *supra* note 7, at 4.

[63] Supplemental Materials is Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46, at 3. EPIC cited complaints with several tools offered to the public by Google, among them Blogger, You Tube, and Google Maps. *Id.* at 7–8.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] FED. TRADE COMM'N, FTC FILE NO. 071-0170, STATEMENT OF FEDERAL TRADE COMMISSION CONCERNING GOOGLE/DOUBLECLICK 1 (2007) [HEREINAFTER FTC STATEMENT CONCERNING GOOGLE/DOUBLECLICK], http://www.ftc.gov/os/caselist/0710170/071220statement.pdf.

[68] *Id*; *see also* 15 U.S.C. § 18 (2008).

[69] FTC STATEMENT CONCERNING GOOGLE/DOUBLECLICK, *supra* note 67, at 2.

company's privacy requirements "could itself pose a serious detriment to competition in this vast and rapidly evolving industry."[70] Thus, the FTC focused on the competitive aspects of the merger, and finding none that would violate the Clayton Act, approved the merger by a four to one vote, with Commissioner Harbour dissenting.[71] Unlike her colleagues, Harbour argued that "if the Commission closes its investigation at this time, without imposing any conditions on the merger, neither the competition nor the privacy interests of consumers will have been adequately addressed."[72]

VI. THE FTC STAFF'S PROPOSED PRINCIPLES FOR BEHAVIORAL TARGETING

The Google-DoubleClick merger created considerable debate among privacy groups, and groups such as the Center for Democracy and Technology ("CDT") requested that the FTC hold a workshop to deal with their privacy concerns over the merger and Google's policies.[73] Critics of the Microsoft-aQuantive and DoubleClick-Google mergers view them as potential threats to privacy due to potential consumer injuries that could occur, such as invasion of privacy by holding sensitive information for lengthy periods of time, leaving consumers potentially vulnerable to searches by law enforcement officers from various countries with no legal authorization, and encouraging other companies to engage in similar behavior that would exacerbate the problem.[74] On November 1st and 2nd of 2007, the FTC hosted a workshop on online behavioral targeting. [75] Named "eHavioral Advertising: Tracking, Targeting, and Technology," the workshop was intended to "bring together consumer advocates,

---

[70] *Id.*

[71] *See* In the Matter of Google/DoubleClick, FTC File No. 071-0170 (Fed. Trade Comm'n, Dec. 20, 2007) (dissenting statement of Comm'r Pamela Jones Harbour), http://www.ftc.gov/os/caselist/0710170/071220harbour.pdf.

[72] *Id.* at 1.

[73] Supplemental Materials is Support of Pending Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 46.

[74] Complaint and Request for Injunction, Request for Investigation and for Other Relief, *supra* note 11, at 10.

[75] Fed. Trade Comm'n., eHavioral Advertising: Tracking, Targeting and Technology, http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml (last visited Feb. 2, 2009).

industry representatives, technology experts, and academics to address consumer protection issues raised by behavioral targeting."[76]

Nine privacy organizations requested the FTC provide needed consumer protections within the behavioral targeting sphere.[77] The FTC identified several key issues that would drive the agenda: consumer knowledge, the necessity of disclosure to consumers, the use and protection of the collected data, and standards that currently protect this data, along with what standards should be used to protect this data.[78] In response to the FTC workshop, several industry groups, consumer advocates, and individual companies created recommendations involving the issues raised by behavioral targeting. Among the recommendations were a "Do Not Track" proposal, reports that discussed and critiqued the current practices in behavioral targeting and self-regulatory initiatives, and a variety of industry initiatives to address the privacy issues raised.[79]

After hosting the workshop and reviewing the comments it generated, the FTC determined that there was a consensus on certain core issues and concerns that had emerged from the discussion.[80] The FTC staff drafted proposed principles from this consensus, which were released for public comments and input on the core issues.[81] The issues involved the lack of knowledge consumers have regarding

---

[76] *Id.*

[77] Press Release, Ctr. for Democracy and Tech., Privacy & Consumer Groups Recommend "Do Not Track List" and Other Policy Solutions to Offer Consumers More Control Over Online Behavioral Tracking (Oct. 31, 2007), *available at* http://www.cdt.org/press/20071031press.php.

[78] *See* ONLINE BEHAVIORAL ADVERTISING, *supra* note 1, at 2.

[79] *Id.* at 2. The requested "Do Not Track" list was intended to protect consumers in the same way that the Do Not Call list does; allowing consumers to express a desire to keep their information from being tracked, stored, and used without their permission or knowledge. Ctr. for Democracy & Tech., *supra* note 77. *See also*, WORLD PRIVACY FORUM, THE NETWORK ADVERTISING INITIATIVE: FAILING AT CONSUMER PROTECTION AND AT SELF-REGULATION (Nov. 2, 2007), http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf. The World Privacy Forum pointed out four particular failings of the current NAI guidelines: lack of a consistently working opt-out cookie, ignorance of new business practices and profiling techniques, a lack of inclusion of a majority of behavioral targeting groups, and a lack of transparency and independence.

[80] ONLINE BEHAVIORAL ADVERTISING, *supra* note 1, at 2.

[81] *Id.*

behavioral targeting; the values of transparency and consumer autonomy, described by business and consumer groups as "critical to the development and maintenance of consumer trust in the online marketplace;" and concerns of data collected for behavioral targeting falling into the wrong hands or being misused.[82]

From these core issues, the FTC then proposed some governing principles for behavioral targeting on the day that the Google-DoubleClick merger was approved, and sought comment by the interested parties.[83] The first issue addressed was that of the interested parties citing a need for greater transparency and consumer control in behavioral targeting.[84] Interest groups criticized current disclosures as being "difficult to understand, inaccessible, and overtly technical and long."[85] In addition, the FTC noted clearer disclosure allows consumers to make informed decisions regarding whether they desire personalized advertising.[86] However, the FTC noted that many consumers do not even read privacy policies, raising a question of how willing and able consumers are to understand long privacy disclosures.[87]

The FTC stated that privacy policies are an important tool for both providing information to consumers as well as promoting accountability among businesses; at the same time, the FTC conceded, businesses may have legitimate needs to change privacy policies.[88] The FTC concluded that companies must keep any promises made at the time data is collected in regard to the handling or protection of

---

[82] *Id.*

[83] *Id.* at 3.

[84] *Id.*

[85] *Id.* The FTC proposed that websites that collected data for behavioral targeting should provide a "clear, concise, consumer-friendly, and prominent statement" that (1) the consumer's online activity data was being collected for behavioral targeting purposes, and (2) consumers can choose whether to have their information collected for such purpose. Additionally, websites were to provide consumers with a "clear, easy-to-use, and accessible method" to exercise whether or not the websites collected their information. *Id.* at 3.

[86] *Id.*

[87] *Id.* For more information on consumer habits regarding privacy policies, see Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 543 (2008) (within this same volume).

[88] ONLINE BEHAVIORAL ADVERTISING, *supra* note 1, at 5.

consumer data, even if policies are later changed.[89] Thus, before companies can use data in a materially different manner than originally suggested, the FTC proposed that affected consumers must provide affirmative, express consent.[90] The second issue tackled was that of the security of the collected data. Individuals and privacy interest groups stated that appropriate security measures were needed in order to ensure that data collected would not fall into the hands of criminals.[91] Still, the FTC noted that some data collected would probably not be traceable to individuals and would thus do little harm even if wrongfully obtained.[92]

Third, there was a discussion of the duration of data retention. While noting that users faced greater risks when collected data was held for long periods of time, the FTC also noted that there could be valid reasons for a company to hold onto such information for extended periods of time, including improving customer service and tracking criminal activities on the website.[93]

Additionally, the FTC noted that consumers might consider the use of sensitive information collected for behavioral targeting to be an invasive use of personal information.[94] Lastly, the FTC discussed their concern that the consumer-tracking data collected for behavioral targeting purposes could be used for purposes that were potentially harmful.[95] The FTC did not propose a remedial principle in regard to this issue, citing a need for additional information.[96]

---

[89] *Id.*

[90] *Id.* at 5–6.

[91] *Id.* at 4. The FTC proposed a "reasonable security" standard for data collected for behavioral targeting, with protection of the data being based on "sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company."

[92] *Id.*

[93] *Id.* The FTC proposal was that information should only be retained as long as necessary to "fulfill a legitimate business or law enforcement need." *Id.* at 4.

[94] *Id.* The FTC's proposed principle to remedy this issue was that companies should only collect sensitive data for the purposes of behavioral targeting when the user from whom they were collecting the data gave affirmative express consent. The FTC sought specific input on what information should be sensitive and whether advertising companies should ever use that sensitive information or whether it should be subject to consumer choice.

[95] *Id.* at 6. This harm was considered especially high in cases where the collection of the data was invisible to consumers, though it was also noted that there was a possibility that

After listing their proposed principles, the FTC sought additional commentary and discussion from the public at large and from those affected by the provisions specifically.[97] In addition, the FTC noted that it did not intend to block additional discussion on other ideas that addressed the issues raised by online behavioral targeting.[98]

VII. COMMENTS RECEIVED BY THE FTC AND THE NEW NAI PRINCIPLES OF 2008

The FTC requested comments on their eHavioral conference, and received sixty-three comments as of January 4, 2009.[99] Among the organizations that have commented are the NAI and the CDT. The NAI noted in their comments that behavioral targeting in and of itself is not harmful.[100] Additionally, the NAI remarked that data used in behavioral targeting is not inherently risky, because the data typically collected is not of a sort that would place persons at risk for identity theft.[101] The NAI also noted that behavioral targeting allows the development and creation of stronger communities of previously disparate, like-minded persons, wherein these persons can coordinate

---

secondary data usage could potentially provide benefits such as the secondary data being used to develop or enhance new or existing products appealing to consumer bases.

[96] *Id.* at 6. In particular, the FTC sought data on (1) the secondary uses of data that raise concern, (2) whether companies were using this concerned data for secondary purposes, (3) "whether the concerns about secondary uses are limited to the use of personally identifiable data or also extend to non-personally identifiable data," and (4) if these secondary uses occur, whether they merit a form of heightened protection.

[97] *Id.*

[98] *Id.*

[99] Fed. Trade Comm'n, # 228; Project No. P859900: Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles, http://www.ftc.gov/os/comments/behavioraladprinciples/index.shtm (last visited Feb. 2, 2009).

[100] Letter from J. Trevor Hughes, Executive Director, Network Adver. Initiative, to Office of the Sec'y, Fed. Trade Comm'n (Apr. 10, 2008), *available at* http://www.ftc.gov/os/comments/behavioraladprinciples/080410nai.pdf.

[101] *Id.* at 5. Data with potential for abuse is data gathered that can personally identify users. The NAI states that NAI group members do not collect personally identifiable information, and the information collected is not subject to the inherent risks of identity theft and other abuses that exist with personally identifiable information. *Id.* at 5–6.

and convene.[102] Still, consumers are concerned about the use of their browsing history in the behavioral targeting context.[103] The NAI recommended that due to the broad and diverse nature of business models in the online economy, the best solution to privacy concerns would be self-regulation by the behavioral targeting companies alongside codes of practice promulgated by organizations such as the American Advertising Federation for advertisers and the Interactive Advertising Bureau for websites.[104]

Additionally, the NAI released updated principles of self-regulation in December of 2008.[105] The NAI required all members to follow their new principles of transparency, notice, choice, use limitations, transfer and service restrictions, access, reliable sources, security, data retention, and following applicable laws, as set out by the NAI.[106] Such principles were stated as continuing the NAI's

---

[102] *Id.* at 7.

[103] *Id.* at 8.

[104] *Id.* at 10. *See also* AAF-Online Privacy, http://www.aaf.org/default.asp?id=358 (last visited Feb. 9, 2009). IAB– Privacy Policy, http://www.iab.net/privacy_policy (last visited Feb. 9, 2009).

[105] NETWORK ADVER. INITIATIVE, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT 1 (2008), http://networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf. The NAI itself was introduced in 1999 after the DoubleClick-Abacus fiasco, adopted its first set of principles in 2000, and updated these principles in 2008. Network Adver. Initiative, The NAI Principles: How They Help Protect Your Privacy, http://networkadvertising.org/managing/principles.asp (last visited Feb. 9, 2009). Press Release, Network Adver. Initiative, Network Advertising Initiative Announces 2008 NAI Self-Regulatory Code of Conduct for Online Behavioral Advertising (Dec. 16, 2008), *available at* http://networkadvertising.org/networks/2008_NAI_Principles_PR_FINAL.pdf.

[106] NETWORK ADVER. INITIATIVE, *supra* note 105, at 4–11. The principles are as follows: (1) Transparency by maintenance of a NAI website, as well as reasonable efforts to inform consumers; (2) notice by clear and conspicuous postings of clear descriptions of several pieces of information having to do with data collection; (3) choice of opt-out options for collection of identification, with mergers of personally identifiable ("PII") and non-personally identifiable information ("non-PII") and collection of sensitive data requiring consumers to opt-in; (4) limiting of use of data to marketing purposes, and of collection of data for companies to those with which there is a contractual relationship; (5) contractual requirements with third parties requiring adherence to the NAI principles for PII and non-PII that will be merged with non-PII; (6) reasonable access to consumers to collected data; (7) members making reasonable efforts to assure they obtain their data from reliable sources; (8) reasonable security measures determined by factors such as data sensitivity and risks faced by companies; (9) data only being retained for legitimate business needs; and (10) members following applicable law. *Id.* at 7–10.

commitment to fair information practices and business models, while still maintaining self-regulation.[107]

Encouraged by the FTC's self-regulation principles, the CDT sent in comments of their own.[108] The CDT declared that the NAI's self-regulatory principles were inadequate in regard to protecting individual consumers. [109] It felt consumer choice benefits far outweighed the costs of following stricter guidelines, and therefore, asked for more specific guidelines than those suggested by the FTC, fearing that the FTC's vague guidelines would be less likely to have a significant impact on protecting consumer privacy.[110] While pleased with most of the FTC's proposed principals, the CDT remained concerned that consumer control and transparency were not treated as the same issue, and that the creation of standards in disclosures of behavioral targeting companies would raise consumer awareness of targeting the associated privacy concerns.[111] The CDT also suggested that the FTC promote further transparency through web browsers and create explicit consumer control options.[112] Consumer opt-out was noted as an option that should be honored until the consumer voluntarily opts back in.[113]

IX. THE FTC'S SELF REGULATORY PRINCIPLES

On February 12, 2009, the FTC released its much-anticipated behavioral targeting principles, opting for a self-regulatory approach. [114] The principles redefine behavioral targeting as the

---

[107] *Id.* at 3.

[108] CTR. FOR DEMOCRACY & TECH., ET AL., IN REGARDS TO THE FTC STAFF STATEMENT: "ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES," (Apr. 11, 2008), http://www.ftc.gov/os/comments/behavioraladprinciples/080411cdtetal.pdf.

[109] *Id.* at 5–6.

[110] *Id.* at 6.

[111] *Id.* at 19.

[112] *Id.* at 18.

[113] *Id.* at 21.

[114] Press Release, Fed. Trade Comm'n, FTC Staff Revises Online Behavioral Targeting Principles (Feb. 12, 2009), *available at* http://www.ftc.gov/opa/2009/02/behavad.shtm. FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE

tracking of consumer online activities over time to deliver advertising services that are targeted to consumer interests.[115] The FTC's report primarily addresses transparency and consumer control, stating that websites should provide clear and concise statements regarding data collection for behavioral profiling, and that consumers should be able to choose whether they desire to have their information collected for such a purpose.[116] The report also suggests that alternative disclosure and opt-out methods should be developed for data collection "outside the traditional website context," whatever that would include.[117]

The FTC then dealt with the security of the collected data. First, FTC staff suggested that the data collected should be reasonable when viewed in regard to the data's sensitivity, the gathering company's business operations, the particular risks the gathering company may face, and the protections considered reasonably available to the company.[118] Companies were also told they should only retain data as long as necessary to fulfill legitimate business needs.[119]

The FTC further stated that companies must honor any prior affirmative promises made regarding their handling and retention of behavioral targeting data.[120] This holds true even if the company later changes its data-retention policies.[121] Were a company to attempt to

---

BEHAVIORAL ADVERTISING 1 (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. Concurring statements as to the regulatory principles were made by Commissioner Pamela Jones Harbour (Concurring Statement of Comm'r Paula Jones Harbour, Regarding Staff Report, "Self-Regulatory Principles for Online Behavioral Targeting" (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadharbour.pdf) and Commissioner Jon Leibowitz (Concurring Statement of Comm'r Jon Leibowitz, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Targeting (Feb. 2009), http://www.ftc.gov/os/2009/02/P085400behavadleibowitz.pdf).

[115] FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, *supra* note 114, at 46. This definition expressly excluded "first party advertising," where no data is shared with third parties. The definition also expressly excluded "contextual advertising," where ads are based upon single visits to a web page or a single search query. *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.* at 46–47.

[119] *Id.* at 47.

[120] *Id.*

[121] *Id.*

use the data in a different manner than originally stated, the FTC would require consumers to give their express affirmative consent to the policy changes.[122] According to the FTC's report, companies may only collect sensitive data for behavioral targeting after receiving express affirmative consent from the user.[123] The FTC noted that its principles are based on a self-regulatory model, and therefore, do not create an affirmative obligation on behavioral targeting companies to abide by the principles.[124]

X. CONCLUSION

Behavioral targeting provides a helpful method of creating personally directed advertisements from the information collected from Internet users, and allows better advertising of niche markets, allowing them to expand and diversify. However, the data behavioral advertising companies collect raises privacy concerns, and mergers between large corporations that house significant amounts of behavioral targeting information heighten concerns over the security and privacy measures placed over such information. While opt-out cookies and self-policing have been the main approach to assure that users' information is given the proper level of security, concerns still exist that this is not enough.

The FTC's newly released self-regulatory principles were revised to deal with the most pressing concerns of privacy advocate groups. However, having only recently been created, it remains unclear whether these principles will be effective or whether Congress will have to step in to provide more rigorous regulations.

---

[122] *Id.*

[123] *Id.*

[124] *Id.* at 45–46.